IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):   Anil V. Rao, Wayne R. Weilnau

Assignee: Dell USA, L.P.

Title: System and Method for Installing System Manufacturer Provided Software

Serial No.:   09/271,581   Filing Date: March 18, 1999

Examiner: Benjamin E. Lanier Group Art Unit: 2132

Docket No.:   DC-01492   Customer No.:   33438

Austin, Texas
April 7, 2006

Mail Stop Appeal Brief - Patents
Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

Applicant submits this Appeal Brief pursuant to the Notice of Appeal and Pre-Appeal Request for Review filed in this case on February 7, 2006. A Notice of Panel Decision from Pre-Appeal Brief Review was mailed on February 21, 2006.

A check is enclosed in the amount of $500.00 for the Appeal Brief fee. The Board is also authorized to deduct any other amounts required for this appeal brief and to credit any amounts overpaid to Deposit Account Number 502264.

I. REAL PARTY IN INTEREST - 37 CFR § 41.37(c)(1)(i)

The real party in interest is the assignee, Dell Products L.P., as named in the caption above and as evidenced by the assignment set forth at Reel 9850, Frame 0771.

II. RELATED APPEALS AND INTERFERENCES - 37 CFR § 41.37(c)(1)(ii)

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal.

- 1 -

III.   STATUS OF CLAIMS - 37 CFR § 41.37(c)(1)(iii)

Claims 1 - 28 are pending in the application. Claims 1 - 28 stand rejected. The rejection of claims 1 - 28 is appealed. Appendix "A" contains the full set of pending claims.

IV.   STATUS OF AMENDMENTS - 37 CFR § 41.37(c)(1)(iv)

No amendments after final have been requested or entered.

V.   SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

The present invention, as set forth by independent claim 1, relates to a method of selectively installing software onto a computer system 110 manufactured by a computer system manufacturer. The method includes reading a configuration file that contains computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer (see e.g., Application, Page 7, lines 11 – 13); determining an encrypted key from one or more bytes from the configuration file including the manufacturer specific identification information (see e.g., Application, Page 7, lines 8 – 18); and, deciphering data stored on a nonvolatile storage device using the key so as to ensure that the software is installed only on a computer system manufactured by the computer system manufacturer (see e.g., Application Page 7, lines 8 – 10 and Page 7, line 29 – Page 8, line 15).

The present invention, as set forth by independent claim 10, relates to a computer system 110 for selectively installing software, the computer system 110 being manufactured by a computer system manufacturer. The computer system 100 includes a processor; nonvolatile memory operatively coupled to the processor; a nonvolatile storage device; one or more configuration files, the one or more configuration files containing computer system information (see e.g., Application, Page 7, lines 11 – 13) and a computer program executable by the processor. The computer system information includes manufacturer specific identification information identifying the computer system manufacturer. The computer program is capable of reading a configuration file stored in the nonvolatile memory and determining an encrypted key from one or more bytes read from the configuration file including the manufacturer specific

identification information. The encrypted key is capable of deciphering data stored on the nonvolatile storage device so as to ensure that the software is installed only on a computer system manufactured by the computer system manufacturer (see e.g., Application Page 7, lines 8 – 10).

The present invention, as set forth by independent claim 18, relates to a method of selectively installing software onto a computer system 110 manufactured by a computer system manufacturer. The method includes reading a configuration file that contains computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer (see e.g., Application Page 7, lines 11 – 13); determining a key from one or more bytes from the configuration file including manufacturer specific information (see e.g., Application, Page 7, lines 15, 16); and, storing the key in a registry file (see e.g., Application, Page 8, lines 5 – 7). Independent claim 20 is relates to a computer readable medium of similar scope to claim 18. Independent claim 22 relates to a computer system of similar scope to method claim 18.

The present invention, as set forth by independent claim 23, relates to a method of installing software onto a computer system 110 manufactured by a computer system manufacturer after a sale of the computer system 110. The computer system includes computer system information including manufacturer specific identification information identifying the computer system manufacturer (see e.g., Application Page 7, lines 11 – 13). The method includes providing encrypted data and an unencrypted setup program to the computer system, the encrypted data including software application files (see e.g., Application Page 7, lines 6 – 9); reading a configuration file that contains the computer system information via the unencrypted setup program (see e.g., Application Page 7, lines 8 – 10); determining an encrypted key from one or more bytes from the configuration file including the manufacturer specific identification information (see e.g., Application Page 7, lines 11 – 13); deciphering the encrypted data stored using the encrypted key so as to ensure that the software application files are installed only on a computer system manufactured by the computer system manufacturer (see e.g., Application Page 7, lines 8 – 10).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL - 37 CFR § 41.37(c)(1)(vi)

Claims 1, 4, 5, 8, 10, 12, 13, 16, 18, 20, 22, 23-28 stand rejected over Kubota, U.S. Patent No. 5,034,980 (Kubota), in view of Patterson, U.S. Patent No. 6,389,541. Claims 2, 11, 19 and 21 stand rejected over Kubota in view of Patterson and in view of Charabaszcz, U.S. Patent No. 6,363,497. Claim 3 stands rejected over Kubota in view of Patterson and Charabaszcz and further in view of Dollahite, U.S. Patent No. 5,748,877. Claims 6 and 14 stand rejected over Kubota in view of Patterson and further in view of Cooper, U.S. Patent No. 5,757,904. Claims 7 and 15 stand rejected over Kubota, in view of Patterson and further in view of Pearce, U.S. Patent No. 5,694,582. Claims 9 and 17 stand rejected over Kubota in view of Patterson and further in view of Saxena, U.S. Patent No. 6,259,449.

VII. ARGUMENT - 37 CFR § 41.37(c)(1)(vii)

Claims 1, 10, 18, 20, 22 and 23 are allowable over Kubota and Patterson

The present invention generally relates to selectively installing software onto a customer's computer system 110 based upon computer system specific information. The computer specific information is included in one or more configuration files. In a Windows™ environment, the configuration files include a BIOS/DOS memory file. Software to be installed is encrypted and stored on a nonvolatile storage medium that may be a CD-ROM, a floppy disk, a fixed disk, or accessed through a Web Page over the Internet. The configuration file is read to locate the computer system specific information and build an encrypted key for deciphering the encrypted software (235). The encrypted software is deciphered 270 and stored on the user's computer 760 (i.e., on the user's fixed disk drive) where it will be operable by the user. Because many software products include many individual software files, the encryption key is stored in a system registry 260 where it is repeatedly retrieved by a setup program performing the deciphering and installing. (See generally Figure 2 and Page 7, Line 5 – Page 9, Line 8.)

In the Examiner's Response to the arguments set forth in the Response filed on October 26, 2005, the Examiner set forth:

Applicant's arguments filed 26 October 2005 have been fully considered but they are not persuasive. Applicant's arguments that the prior art does not disclose software being installed is after sale software provide by a computer system manufacturer after the sale of a computer system and that the deciphering of data is to ensure that the after sale software provided by the computer system manufacturer after sale of the computer system is installed only on a computer system manufactured by the computer system manufacturer is not persuasive because *it would be an inherent feature of this combination to have the installation procedure of the above combination occur after the sale of the computer system because Kubota discloses that the identification information/key is hardcoded in the microprocessor implemented in BIOS information at the time of manufacture.* Therefore, the software installation procedure disclosed in Kubota would occur after the computer system has been sold. If the software were to be installed before the sale of the computer system, the software would have been installed at the time of manufacture along with the hardcoding of the identification information/key in the microprocessor or implementation in BIOS information. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the computer software that is installed in the copy protection system of the combination disclosed by The Board because the manufacturer of the computer systems would keep their identification/keying information secret and would therefore themselves encrypt the software to be distributed to their computer systems for installation. Keeping their identification/keying information secret would help prevent users of the manufacturer's computer systems from mistakenly installing computer software provided by other manufacturers (Final Office Action, November 07, 2005 Pages 2 – 3, emphasis added).

When discussing the Decision from the Board of Patent Appeals Decision mailed on August 30, 2005, the Examiner set forth:

>   With respect to the combination made by the Board above, it would be an inherent feature of this combination to have the installation procedure of the above combination occur after the sale of the computer system because Kubota discloses that the identification information/key is hardcoded in the microprocessor or implemented in BIOS information at the time of manufacture. Therefore, the software installation procedure disclosed in Kubota would occur after the computer system has been sold. If the software were to be installed before the sale of the computer system, the software would have been installed at the time of manufacture along with the hardcoding of the identification information/key in the microprocessor or implementation in BIOS information. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the computer software that is installed in the copy protection system of the combination disclosed by The Board because the manufacturer of the computer systems would keep their identification/keying information secret and would therefore themselves encrypt the software to be distributed to their computer systems for installation. Keeping their identification/keying information secret would help prevent users of the manufacturer's computer systems from mistakenly installing computer software provided by other manufacturers.

However, this argument does not appreciate that or take into consideration that the claim limitations that set forth that the after sale software is provided *by the computer system manufacturer* and that the after sale software is installed *only* on a computer system manufactured by the computer system manufacturer as substantially required by each independent claim. Applicants maintain that this feature is neither directly nor inherently disclosed by the cited references.

Kubota discloses a microprocessor which provides copy protection. The microprocessor includes an integrated decoding circuit having a unique cryptographic code for providing copy protection of protected computer software (Kubota, Col. 2, lines 62 – 65.) When a microprocessor is manufactured, a key associated with an ID of the microprocessor is embedded into the decoder. (Kubota, Col 3, line 67 – Col. 4, line 1.) When copy protection of software is desired, the software is encrypted to function uniquely with the microprocessor. (Kubota, Abst.)

More specifically, Kubota sets forth:

> The integrated circuit microprocessor chip of the present invention has integrated within it a deciphering code and a decoding circuit to decode the cryptographically protected software. For each individual chip a unique key (or code) is embedded as part of the decoding circuit during the fabrication of the chip. This key operates to decipher the coded software. Computer software which is to be copy protected is cryptographically coded such that only a unique key can decipher the software. That is, the computer software is coded according to the key value of a particular chip and can operate properly only with the chip having that key. Therefore, there is a one-to-one relationship between a copy protected computer software and a given microprocessor.

> In operation, when the software is to be obtained by the computer user, the user must identify to the supplier of the software the identification of the user's specific microprocessor. An identification number (ID) is attributed to each microprocessor. Once the software provider is given an ID, the software supplier will then encrypt the software according to the code associated with that ID. Then this software is provided to the user. When the copy protected software is accessed by the appropriate microprocessor having that ID, the key provides the correct deciphering. However, if the key value is incorrect, indicating that the software is not intended for that microprocessor, then the correct deciphering cannon occur. (Kubota, Col., 3, lines, 22 – 50.)

Kubota discloses and relates solely to microprocessors. Kubota does not provide any disclosure relating to computer systems, much less to identifying a particular computer system manufacturer. Applicants respectfully submit that providing manufacturer specific identification

information identifying a computer system manufacturer is patentably distinct from uniquely identifying a particular microprocessor as disclosed in Kubota. Accordingly, Kubota does not teach or suggest all of the claim limitations of the claimed invention. (See M.P.E.P. 2143.03.)

Patterson discloses a method for regulating access to digital content such as text, video and music. The content is stored as part of a compressed and encrypted data file at a client computer. The content is inaccessible to the user until a use authorization occurs. The data file is activated and locked to the particular client computer. The data file is not accessible without new authorization if the data file is transferred to another computer.

Kubota and Patterson do not provide any disclosure relating to computer systems, much less to identifying a particular computer system manufacturer such that after sale software provided *by the computer system manufacturer* and after sale software is installed *only* on a computer system manufactured by the computer system manufacturer as substantially required by each independent claim. Applicants respectfully submit that providing manufacturer specific identification information identifying a computer system manufacturer to enable these features is patentably distinct from uniquely identifying a particular microprocessor as disclosed in Kubota. The deficiencies of Kubota are not completed by Patterson. As with Kubota, Patterson provides no disclosure relating to providing manufacturer specific information identifying a computer system manufacturer to as to ensure that after sale software is installed only on a computer system manufactured by the computer system manufacturer, as substantially required by claims 1, 10, 18, 20 and 22. Accordingly, claims 1, 10, 18, 20 and 22 are allowable over Kubota and Patterson.

More specifically, neither Kubota or Patterson disclose or suggest a method of selectively installing software onto a computer system manufactured by a computer system manufacturer where the method includes reading a configuration file that contains computer system information including manufacturer specific identification information *identifying the computer system manufacturer* and deciphering data stored on a nonvolatile storage device using the key so *as to ensure that the software is installed only on a computer system manufactured by the computer system manufacturer*, as required by independent claim 1. Accordingly, independent

claim 1 is allowable over Kubota and Patterson. Claims 2 – 9 and 24 depend from claim 1 and are allowable for at least this reason.

Additionally, neither Kubota or Patterson disclose or suggest a computer system for selectively installing software on a computer system manufactured by a computer system manufacturer where the computer system includes a computer program which determines an encrypted key from one or more bytes read from the configuration file, the encrypted key being capable of deciphering data so as to ensure that the software *is installed only on a computer system manufactured by the computer system manufacturer* and the *computer system information includes manufacturer specific identification information identifying the computer system manufacturer*, as required by independent claim 10. Accordingly, independent claim 10 is allowable over Kubota and Patterson. Claims 11 – 17 and 25 depend from claim 10 and are allowable for at least this reason.

Additionally, neither Kubota nor Patterson disclose or suggest selectively installing software onto a computer system manufactured by a computer system manufacturer where the method includes reading a configuration file that contains computer system information where the computer system information includes *manufacturer specific identification information identifying the computer system manufacturer*, as required by independent claims 18, 20 and 22. Accordingly, independent claims 18, 20 and 22 are allowable over Kubota and Patterson. Claims 19 and 26 depend from claim 18 and is allowable for at least this reason. Claims 21 and 27 depend from claim 20 and is allowable for at least this reason. Claim and 28 depends from claim 22 and is allowable for at least this reason.

Additionally, neither Kubota or Patterson disclose or suggest a method of installing software onto a computer system manufactured by a computer system manufacturer after a sale of the computer system where *the computer system includes computer system information including manufacturer specific identification information identifying the computer system manufacturer* and the method includes *providing encrypted data and an unencrypted setup program to the computer system*, the encrypted data including software application files, reading *a configuration file that contains the computer system information via the unencrypted setup program*, determining an encrypted key from one or more bytes from the configuration file

including *the manufacturer specific identification information*, and deciphering the encrypted data stored using the encrypted key *so as to ensure that the software application files are installed only on a computer system manufactured by the computer system manufacturer*, as required by independent claim 23. Accordingly, independent claim 23 is allowable over Kubota and Patterson.

VIII. CLAIMS APPENDIX - 37 CFR § 41.37(c)(1)(viii)

A copy of the pending claims involved in the appeal is attached as Appendix A.
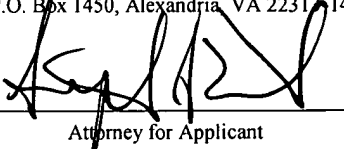
IX. EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None

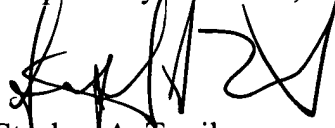## X. RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.

XI. CONCLUSION

For the reasons set forth above, Applicant respectfully submits that the rejection of pending Claims 1 - 28 is unfounded, and requests that the rejection of claims 1 - 28 be reversed.

<table>
<tr><td>
I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Board of Patent Appeals and Interferences, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450, on April 7, 2006.

_____ ___4/7/06___
Attorney for Applicant   Date of Signature
</td></tr>
</table>

Respectfully submitted,

Stephen A. Terrile
Attorney for Applicant
Reg. No. 32,946

1.   A method of selectively installing software onto a computer system manufactured by a computer system manufacturer, said method comprising:

      reading a configuration file that contains computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer;

      determining an encrypted key from one or more bytes from the configuration file including the manufacturer specific identification information;

      deciphering data stored on a nonvolatile storage device using the key so as to ensure that the software is installed only on a computer system manufactured by the computer system manufacturer.

2.   The method, as recited in claim 1, wherein the configuration file includes a BIOS memory file.

3.   The method, as recited in claim 2, wherein the BIOS memory file is stored in nonvolatile memory connected to the computer system.

4.   The method, as recited in claim 1, further comprising:
storing the key in a registry file.

5.   The method, as recited in claim 1, further comprising:
copying the deciphered data onto another nonvolatile storage device connected to the computer system.

6.   The method, as recited in claim 1, further comprising:
checking the authenticity of the key.

7.   The method, as recited in claim 1, wherein the reading and the determining are performed by a software program stored in a dynamic linked library.

8.   The method, as recited in claim 1, wherein the nonvolatile storage device includes:

a CD-ROM device; and

a CD-ROM.

9.   The method, as recited in claim 1, wherein the nonvolatile storage device stores the data on a Web Page that is accessible on a global computer network.

10.   A computer system for selectively installing software, the computer system being manufactured by a computer system manufacturer, the computer system comprising:

a processor;

nonvolatile memory operatively coupled to the processor;

a nonvolatile storage device;

one or more configuration files, the one or more configuration files containing computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer;

a computer program executable by the processor, wherein the computer program is capable of reading a configuration file stored in the nonvolatile memory, determining an encrypted key from one or more bytes read from the configuration file including the manufacturer specific identification information;

wherein the encrypted key is capable of deciphering data stored on the nonvolatile storage device so as to ensure that the software is installed only on a computer system manufactured by the computer system manufacturer.

11.   The computer system, as recited in claim 10, wherein the configuration file includes a BIOS memory file.

12.   The computer system, as recited in claim 10, further comprising:

a second nonvolatile storage device; and

a registry file stored on the second nonvolatile storage device;

wherein the encrypted key is stored in the registry.

13.   The computer system, as recited in claim 10, further comprising:

a second nonvolatile storage device that stores the deciphered data.

14.   The computer system, as recited in claim 10, wherein the computer software is further capable of checking the authenticity of the encrypted key.

15.   The computer system, as recited in claim 10, wherein the software program is located in a dynamic linked library.

16.   The computer system, as recited in claim 10, wherein the nonvolatile storage device includes:

a CD-ROM device; and

a CD-ROM.

17.   The computer system, as recited in claim 10, wherein the nonvolatile storage device stores the data on a Web Page that is accessible on a global computer network.

18.   A method of selectively installing software onto a computer system manufactured by a computer system manufacturer, said method comprising:

reading a configuration file that contains computer system information, the computer

system information including manufacturer specific identification information

identifying the computer system manufacturer;

determining a key from one or more bytes from the configuration file including

manufacturer specific information;

storing the key in a registry file.

19.   The computer readable medium, as recited in claim 18, wherein the configuration file includes a BIOS memory file.

20.   A computer readable medium for selectively installing software onto a computer system manufactured by a computer system manufacturer, the computer readable medium comprising:

means for reading a configuration file that contains computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer;

means for determining a key from one or more bytes from the configuration file including the manufacturer specific identification information;

means for storing the key in a registry.

21.   The computer readable medium, as recited in claim 20, wherein the configuration file includes a BIOS memory file.

22.   A computer system for selectively installing software onto a computer system manufactured by a computer system manufacturer, the computer system comprising:

means for reading a configuration file that contains computer system information, the computer system information including manufacturer specific identification information identifying the computer system manufacturer;

means for determining a key from one or more bytes from the configuration file including the manufacturer specific identification information;

means for storing the key in a registry.

23.   A method of installing software onto a computer system manufactured by a computer system manufacturer after a sale of the computer system, the computer system including computer system information including manufacturer specific identification information identifying the computer system manufacturer, said method comprising:

providing encrypted data and an unencrypted setup program to the computer system, the encrypted data including software application files;

reading a configuration file that contains the computer system information via the unencrypted setup program;

determining an encrypted key from one or more bytes from the configuration file including the manufacturer specific identification information;

deciphering the encrypted data stored using the encrypted key so as to ensure that the software application files are installed only on a computer system manufactured

by the computer system manufacturer.

24.   The method of selectively installing software of claim 1 wherein
the reading, determining and deciphering are performed via a setup program.

25.   The computer system of claim 10 wherein
the computer program includes a setup program, the setup program performing the
reading and determining.

26.   The method of selectively installing software of claim 18 wherein
the reading, determining and deciphering are performed via a setup program.

27.   The computer readable medium of claim 20 further comprising
a setup program, the setup program including the means for reading the configuration file
and the means for determining the key.

28.   The computer system of claim 22 further comprising
a setup program, the setup program including the means for reading the configuration file
and the means for determining the key.

EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None

RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.